Applied Computer Systems
ISSN 2255-8691 (online)
ISSN 2255-8683 (print)
December 2022, vol. 27, no. 2, pp. 101–109
https://doi.org/10.2478/acss-2022-0011
https://content.sciendo.com

Using a Fuzzy-Bayesian Approach for Predicting the QoS in VANET

Hafida Khalfaoui[1*], Abdellah Azmani[2], Abderrazak Farchane[3], Said Safi[4]
[1,3,4]*LIMATI Laboratory, Sultan Moulay Slimane University, Beni Mellal, Morocco*
[2]*Intelligent Automation Laboratory, Abdelmalek Essaadi University, Tetouan, Morocco*

***Abstract* – There are considerable obstacles in the transport sector of developing countries, including poor road conditions, poor road maintenance and congestion. The dire impacts of these challenges could be extremely damaging to both human lives and the economies of the countries involved. Intelligent Transportation Systems (ITSs) integrate modern technologies into existing transportation systems to monitor traffic. Adopting Vehicular Ad-hoc Network (VANET) into the road transport system is one of the most ITS developments demonstrating its benefits in reducing incidents, traffic congestion, fuel consumption, waiting times and pollution. However, this type of network is vulnerable to many problems that can affect the availability of services. This article uses a Fuzzy Bayesian approach that combines Bayesian Networks (BN) and Fuzzy Logic (FL) for predicting the risks affecting the quality of service in VANET. The implementation of this model can be used for different types of predictions in the networking field and other research areas.**

***Keywords* – Bayesian network, fuzzy-Bayesian, fuzzy logic, prediction, quality of service, risk analysis, VANET.**

I. Introduction

VANET is a Mobile Ad-hoc Network (MANET) subclass. Its objective is to create a communication system for Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Infrastructure to-Infrastructure (I2I) that increases awareness in the route and allows acquiring real-time traffic events, such as accidents, pre-crash warnings and emergency electronic brake lights [1], [2]. The mobile nodes are smart vehicles supplied with flexible computing resources containing computers, geolocation systems (GPS), radars, network devices and various sensors [3]. These vehicles are interconnected and can have an interface that allows the driver to receive and send messages to various network entities. Furthermore, they incorporate a positioning device such as GPS and sensors that detect changed conditions, such as the state of the trailer's doors (open or closed), the temperature inside, violent movements and non-programmed stops [4]. These characteristics give high visibility and control of different operations and activities that occur within the transportation and help predict risks and make right decisions.

This paper aims at measuring the quality of service (QoS) in VANET by implementing a Fuzzy-Bayesian (FB) approach. The latter starts by analysing the risks of VANET in order to implement a tool for predicting problems that disrupt the proper functioning of the network. Therefore, this approach allows studying the influence of input parameters, including routing, security and data processing, on the QoS in VANET. After that, the risk can be resolved or even eliminated to safeguard system connectivity and avoid the problems of disruption in the transport, generating additional costs, distribution delays and ultimately dissatisfaction.

The remainder of this article is structured as follows: Section II shows the challenges of VANET. Section III presents the literature related to the QoS in VANET. Section IV explains the construction of the FB model. Section V discusses the approach proposed. The final section concludes this work and presents some future areas of research.

II. Challenges of VANET

Significant problems appear when using ad-hoc communication between vehicles moving in a road environment. The key challenges are as follow:

A. Routing Problems

The routing protocol that establishes and maintains routes from source to destination is the most challenging issue in VANET [5]. Since the infrastructure of VANET is limited, the routing mechanism must be executed by the vehicles themselves, and the intermediate route packets sent between distant vehicles [6]. This mechanism suffers from many issues due to the unique features of VANET, such as the dynamic topology caused by high mobility of vehicles and variable network density. Furthermore, the cars may join and quit the network rapidly, causing frequent path disruption. Consequently, developing an efficient protocol that keeps a route is difficult [7]. Besides, some nodes act selfishly and refuse to participate in the routing to save their resources, such as storage and processing time [6], which can degrade and harm the performance of the network [7]. There are additional issues regarding the VANET routing protocols. The most common are: the scalability and limited bandwidth leading to congestion and interference in the network [8], signal transmission attenuations caused by adverse weather and obstacles, also security issues caused by malicious nodes that can launch

* Corresponding author's e-mail: hafidakhalfaoui1996@gmail.com

©2022 Hafida Khalfaoui, Abdellah Azmani, Abderrazak Farchane, Said Safi.
This is an open access article licensed under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0).

diverse attacks, such as a black hole, eavesdropping, wormhole and rushing attacks [9].

B. Security Problems

The security aspect is an important pillar in VANET. If an attacker arrives to launch an attack, it can have a significant impact on network operations and services. Passive attacks, such as listening to the communication and using the secret data to execute malicious activities, or active attacks, such as removing, modifying, or repeating messages to disrupt the network, are both possible. It can also program traffic signals to cause traffic jams or block streets [10]. VANET presents several security issues because of its unique characteristics, such as the open network environment and dynamic network topology [11]. The following are the most notable security threats.

Authentication

In VANET, there are two types of authentication: identity authentication, which determines the legitimacy of nodes, and message authentication, which prevents fraudulent transmission of messages in the network. Several existing authentication algorithms have solved some security problems in VANETs, but their security still needs improvement. Impersonation, identity (ID) disclosure attacks, spoofing attacks, etc., are types of authentication attacks. They are generated when malicious nodes can create false identities or reveal other node identities to act as legitimate vehicles and benefit from or reinforce incorrect data in the network. For example, an attacker may pretend to be an emergency vehicle in order to slow down other cars [12].

Privacy Protection

Privacy protection has extended concern for VANET. Vehicles in contact with it typically share messages without any privacy or security, which means the message is not encrypted and contains vehicle ID, speed, location and other specific information that is usually linked to the driver's identity. If these private data are open to attackers, this latter can use them to profile users or launch various attacks, such as masquerading and impersonation attacks that can mislead other vehicles and endanger road safety [13], [14].

Confidentiality

Confidentiality is a necessary security requirement for exchanging safety and non-safety messages between vehicles. The message content should be secure and inaccessible to non-authenticated users. Confidentiality also prevents malicious activities, such as man-in-the-middle and traffic analysis attacks [15], [16].

Integrity

Data integrity is one of the VANET security services that focus on conserving and ensuring the precision and accuracy of data during their transmission. There are numerous ways in which the data integrity service can be compromised. The most common data integrity threats are replay, message tampering and illusion attacks [17].

Availability

Availability is a critical factor that aims at protecting the life of users in VANET. It ensures that the network is operational and useful information is always available [18]. The most famous availability threats are denial of service (DOS) attacks, jamming attacks, malware attacks, greedy behaviour attacks, spamming attacks and so on. Their common goals are to use the bandwidth unnecessarily to cause voluntary collisions, decrease communication quality between vehicles and thus interrupt services or prohibit other nodes from using VANET support and services [17].

C. Data Processing Problems

In recent years, the VANET environment has been generating massive amounts of data due to sensor and communication technologies. These data are very important in improving productivity, travel comfort, transportation safety and modern society's economic prosperity. As the amount of data generated by VANET grows exponentially, its complexity and processing will present immense challenges due to the lack of intelligent systems that manage the large quantities of data generated.

As a result, VANET requires complementary technologies to help optimize and efficiently process all data collected from disparate sources. Big data and artificial intelligence (AI) provide competitive advantages in this context, allowing organisations to make better decisions, while reducing operational time and costs. However, these technologies present significant challenges in terms of energy, node storage capacity and computation costs [19]. With the recent emergence of new integrated architectures and access technologies, the computation burden of IA algorithms and big data can be alleviated by migrating complex computations to external cloud servers [20]. This solution also presents some problems in terms of time and security. When the scalability of nodes increases, the existing cloud computing can hardly satisfy the needs of end users. In general, uploading to and downloading from the cloud consume time and energy [21].

III. Related Work

QoS measures the service degree of satisfaction as presented to the end user. In telecommunication networks, QoS aims at achieving better communication behaviour by routing the packets correctly and using resources optimally [22].

Providing QoS support to VANET is an active research area. This network has particular features, such as high mobility, scalability, a lack of centralized control unit, a hidden node issue, limited resources and an insecure medium, which make QoS provisioning very complex.

In VANET, each application has specific QoS requirements; for example, a safety application should have a minimum End-to-End Delay (E2ED) and packet loss because if a warning message does not arrive at a destination quickly, it will not help prevent an accident [23].

In the literature, many efforts and studies are dedicated to the factors that affect the QoS in VANET and the majority are looking into the routing aspect.

The authors of [24] proposed QMM-VANET to maintain security and connectivity in the VANET. It is a clustering routing protocol that considers QoS requirements and mobility constraints. Firstly, this protocol calculates the QoS value of each vehicle and chooses a trustworthy one as the cluster head. Then, it selects gateways among neighbouring nodes and uses a gateway recovery algorithm to pick another gateway if link fails. In comparison to other protocols, this one demonstrated its efficacy in terms of packet delivery ratio and E2ED in the highway scenario.

In [25] and [26], the authors conduct brief analyses on QoS, which include some types of routing protocols that help minimize delay and increase overall QoS in VANET. The authors of [27] also improved various QoS parameters for various scenario networks, such as delay, jitter, throughput and packet loss ratio, by employing various routing algorithms with different mobility patterns, adaptive modulation, multiple-input multiple-output (MIMO) and coding (AMC) techniques.

In [28], the authors exploit Road Side Units (RSUs) to accumulate and transmit traffic data. They attempt to find the shortest route to the destination based on the cost of each transmission path using an effective algorithm called Dijkstra's Dedicated Short Range Communication (DDSRC).

According to the authors of [29], if the number of packets transmitted in the network increases, a queue of packets may be created in the vehicle, and the response time of some packets may expire before being processed, causing a decreased service rate. They attempted to improve VANET performance by removing useless or unused packets, in contrast to related works that investigated the increasing service rate by changing the parameters and properties of scheduler algorithms.

In overall, it can be concluded that none of the previous QoS solutions met all of the QoS criteria.

IV. Modelling the Risk of QoS in VANET Using a Fuzzy-Bayesian Approach

A Bayesian Network (BN) is a probabilistic graphical model developed by Pearl to aid in reasoning under uncertainty [30]. BN is defined by a pair (G, O) with $G = V$, A is a directed acyclic graph that encodes a joint probability distribution over a finite set of categorical variables V, and the arcs A represent direct relationships between them [31]. In addition, a set of parameters O defines the behaviour of each variable caused by its parent in the graph.

In this study, this tool allows for the prediction of problems that disturb the proper functioning of the network by studying the influence of input parameters on such problems. For example, what is the impact of mobility and density on the E2ED of data transmission and, consequently, on the routing quality in the network?

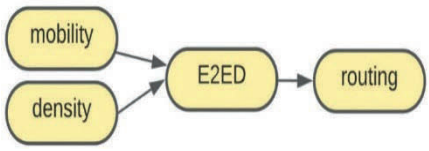


Fig. 1. Example of a causal relationship.

Fig. 1 represents a hierarchical arrangement, with both mobility and density are being ancestors and parents of E2ED; analogical routing is its descendant and its child.

This study started with exhaustive research to identify the main challenges of a VANET network as follows:

- Risks related to data routing influenced by the route conditions, such as mobility, density of nodes and security attacks.
- Risks related to the security of the data circulated in the network due to the lack of robust mechanisms, such as authentication, confidentiality, privacy and integrity.
- Risks related to data processing facilitating to make decisions in the different activities. Processing is affected by the quality and quantity of data collected from the different entities of the network.

This study also identified all the parameters that could influence the occurrence degree of the above-mentioned risks. This identification led to conceiving the nature of the dependencies between the different events and defining the causal architecture of the Bayesian model. The following steps are proposed for the analysis of QoS in VANET developed by the BN:

Step 1: Define the architecture of the BN (causal graph).

Step 2: Generate conditional probabilities of intermediate effects and final impacts.

A. Architecture of the Bayesian Network of QoS in VANET

The architecture of the BN is based on the identification of the relations between the nodes constituting the graph, which is divided according to their typology into three classes:

- The input parameters of the graph: these parameters represent the input nodes of the network.
- Intermediate effects: the direct effects that are broken down into input parameters that are the origin of the causes.
- Final impacts: the factors that directly influence the QoS in VANET.

The investigation of the various factors that influence QoS in VANETs aids in identifying input parameters, as described in Table I, and intermediate effects and final impacts, as shown in Table II. The causal graph in Fig. 2 is developed based on the two tables and after studying the nature of the causal dependencies between them.

B. Generation of Conditional Probabilities of Intermediate Effects and Final Impacts

After constructing the BN graph, the conditional probabilities (CPs) for each variable must be computed. There are numerous sources of probabilistic information available, such as databases[2] containing road traffic and attacks. In this study, the BN considers a large number of parameters that make the existence of a complete database a difficult task. Unfortunately, the available databases are private and insufficiently rich to permit a reliable examination of the

[2] https://www.unb.ca/cic/datasets/index.html

needed probabilities [47]. Therefore, FL is proposed for generating these CPs systematically. It is an effective solution for handling imprecise data and linguistic problems. Its strength lies in its resemblance to human reasoning and natural language.

TABLE I

DESCRIPTION OF THE INPUT PARAMETERS OF THE CAUSAL GRAPH

CATEGORY OF VARIABLES	VARIABLE NAME	DESCRIPTION
Security	Authentication	It represents the mechanism used to provide authenticity of both the data origin and also verify its sender.
	Integrity	It represents the mechanism used to ensure that a sent message should reach the destination on the chosen path without any alteration [32].
	Confidentiality	The mechanism ensures that only authorized users can access the data. Failure to meet this requirement compromises the security of the exchanged data and the privacy of users [33].
	Privacy	This mechanism guarantees the anonymity of drivers and prevents an unauthorized party from knowing the combination between the sender's real identity and private information related to traffic messages, such as vehicle identity, direction and location [34].
	Inadvertence	It refers to threats that result from trusted insiders who do not have malicious intent but fail to manage security responsibly. As a result, a malicious outsider is frequently able to use the privileges of the inattentive insider to carry out security problems.
	Selfish behaviour	It refers to selfish nodes in the network that may refuse to cooperate in forwarding messages in order to increase their own resources [35].
Routing	Mobility	It refers to the movement of nodes communicating wirelessly and varies in function of their speed.
	Density	It is the number of vehicles driving concurrently on the road [36].
	Type of protocol	The routing protocol is used to maintain links in the network to perform packet forwarding. In the VANET, there are many types of routing protocols. Choosing an effective one is very difficult because it depends on various parameters, such as mobility model, environment and others [37].
	Bandwidth	It is the maximum throughput at which packets can be transmitted between nodes without disrupting any existing network flow [38].
	Frequency	It is the number of occurrences of a repeating event per unit of time. If the frequency is high, we get short-range communication, which results in poor connectivity [39].
	Obstacle	Things that can diffract or block the signals in the road, such as buildings, trees, hills and bridges [40].
	Weather	Adverse weather conditions provide a signal transmission attenuation, like rainy or snowy days and dusty weather. Therefore, they will negatively influence the connectivity of high-speed data links in the vehicle communication range [41].
Data processing	Internet	Amount of data uploaded from the internet that can improve the productivity, travel comfort and modern society's economic prosperity.
	OBU	Amount of data exchanged with OBU. It concludes V2V and V2I communications.
	Sensors	Amount of data collected from sensor systems related to state of vehicle or the external environment (based on radar systems, video cameras, image processing, etc.) [42].
	Type of processing	It is critical to choose the suitable type of data processing to avoid negative effect on the data output or the final product.
	Device resources	These are resources/components that allow vehicle to act as a mobile service provider of sensing, data storage, data relaying, computing, infotainment and localization services [43].

TABLE II

DESCRIPTION OF INTERMEDIATE EFFECTS AND FINAL IMPACTS

INTERMEDIATE EFFECTS	DESCRIPTION
Signal transmission	It represents the quality of signal used to transmit data between nodes.
Interference	Interference is caused by any signal other than the one configured in the network, and it obstructs the network normal operation. It usually causes slower speeds, higher latency, frequent disconnects, and sometimes, a complete failure to connect.
Congestion	This variable describes the state of the network when there is an overload of the links, which progressively affects the network performance with an increase in the transmission delay and a decrease in throughput [44].
Connectivity	This property ensures successful data transmission from a source vehicle to a destination. It can be obtained if the number of active vehicles is increased in the network [45].
E2ED	The time required to send a packet from its origin to its destination [46].
Packet loss	The number of packets that fail to reach their destination.

Attacks	It represents the number of attacks launched in the network.
Security	It represents the level of security in the network.
Data processing	Data processing is the process of collecting data and converting it into usable information (graphs, documents, etc.), to be interpreted by computers using various AI algorithms. This variable represents the quality of data processing used in the VANET.
Quantity of data	The amount of data generated in the network due to sensor and communication technologies.
FINAL IMPACTS	DESCRIPTION
Routing	This variable represents the quality of routing that has a great effect in the transmission of data between nodes.
Quality of data	Data quality is determined by many factors such as accuracy, completeness, confidentiality, validity, uniqueness and timeliness.
QoS in VANET	QoS measures the service degree of satisfaction as presented to the end user in the VANET.

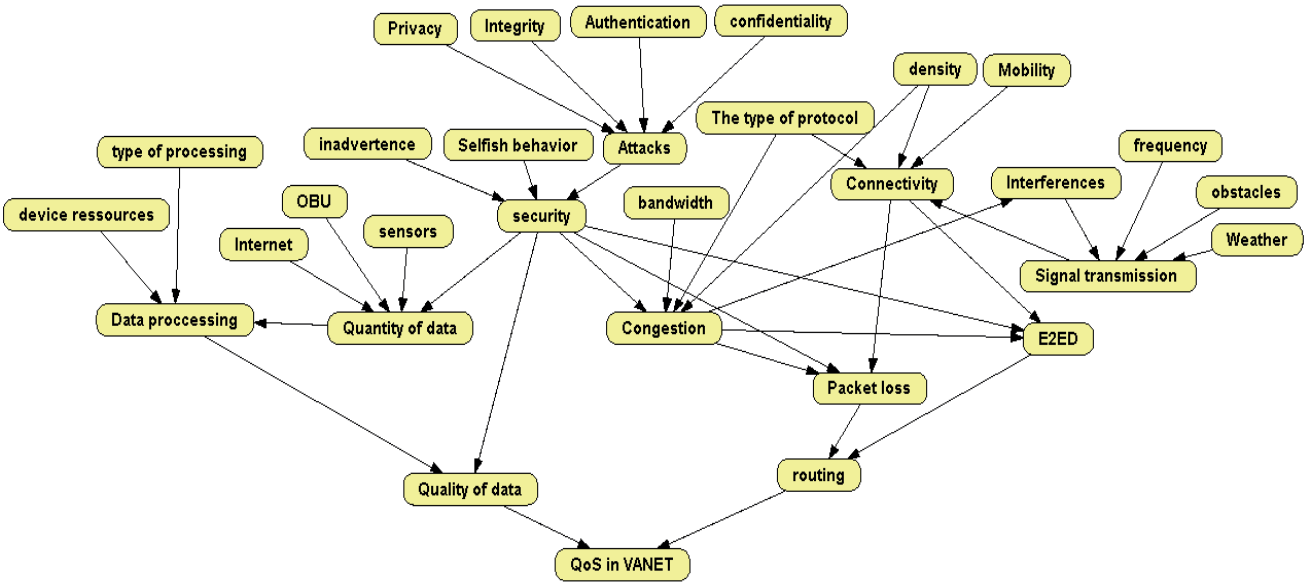


Fig. 2. BN modelling the analyses of risk of QoS in VANET.

The implementation of the FL for generating CPs is done in three principal steps [48], [49]:

- Fuzzification: converts the input variables into a fuzzy subset using fuzzy linguistic values and membership functions.
- Inference: evaluates and combines the fuzzy rules to form conclusions that give the fuzzy outputs of the system.
- Defuzzification: transforms the conclusions provided by the inference engine into numeric values representing the final response of the fuzzy system.

The most widely used inference methods are these of Mamdani [50] and Sugeno [39]. The main difference between them lies in the way the crisp output is obtained from the fuzzy inputs. Mamdani uses a defuzzification technique of fuzzy outputs, while Sugeno uses a weighted average to calculate the result values [51]. This study chooses the method of Sugeno because it has a better processing time. As a result, generating CPs is done just with two first steps.

Fuzzification

To implement the fuzzification step, the fuzzy variables and their linguistic values are presented in Table III.

TABLE III
STATES OF THE BN NODES

VARIABLE	LINGUISTIC VALUES
Authentication	Robust, medium, weak
Integrity	Robust, medium, weak
Confidentiality	Robust, medium, weak
Privacy	Robust, medium, weak
Inadvertence	High, medium, low
Attacks	High, medium, low
Selfish behaviour	High, medium, low
Security	Good, medium, bad
Frequency	High, medium, low
Bandwidth	Large, medium, small
Congestion	High, medium, low
Mobility	High, medium, low
Density	High, medium, low
Interferences	High, medium, low
Obstacle	Many, medium, few
Weather	Good, medium, bad

Type of protocol	Good, medium, bad
Signal transmission	Good, medium, bad
Connectivity	Good, medium, bad
E2ED	Long, medium, short
Packet loss	High, medium, low
OBU	Large, medium, small
Sensors	Large, medium, small
Internet	Large, medium, small
Quantity of data	Large, medium, small
Type of processing	Good, medium, bad
Devices resources	High, medium, limited
Data processing	Good, medium, bad
Quality of data	Good, medium, bad
Routing	Good, medium, bad
QoS in VANET	Good, medium, bad

The membership function is the graph representing the amplitude of each input participation. The rules use the input membership values as a reference to determine their impact on the final outputs [52].

In this work, the Gaussian type is chosen for all the nodes of the BN because it provides less errors in the prediction of the data compared to the others, notably the triangular and trapezoidal forms [53]. Fig. 3 shows an example of this function for the 'routing' variable.

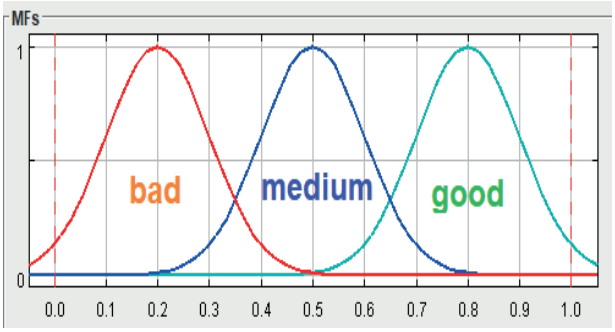


Fig. 3. Membership function for routing variable.

Inference

In the remaining steps, we will assume that all CPs have been generated and the method used will be explained for the node 'QoS in VANET'. In this case, the inference mechanism aims at calculating the table of CPs of this variable while considering all combinations of its parents: 'routing' and 'quality of data'. Table IV presents the set of fuzzy rules used in this example.

The open-source software Fispro[3] is used to implement the fuzzy inference, which provides exact values from different subsets of the output variables. Fig. 4 presents the inference of the variable 'QoS in VANET' knowing that 'data quality' is medium and 'routing' is good, which corresponds to rule 3 in Table IV.

TABLE IV
STATES OF THE BN NODES

RULE	IF QUALITY OF DATA	AND ROUTING	THEN QOS IN VANET
1	medium	bad	bad
2	medium	medium	medium
3	medium	good	medium
4	bad	bad	bad
5	bad	medium	bad
6	bad	good	bad
7	good	bad	bad
8	good	medium	medium
9	good	good	good

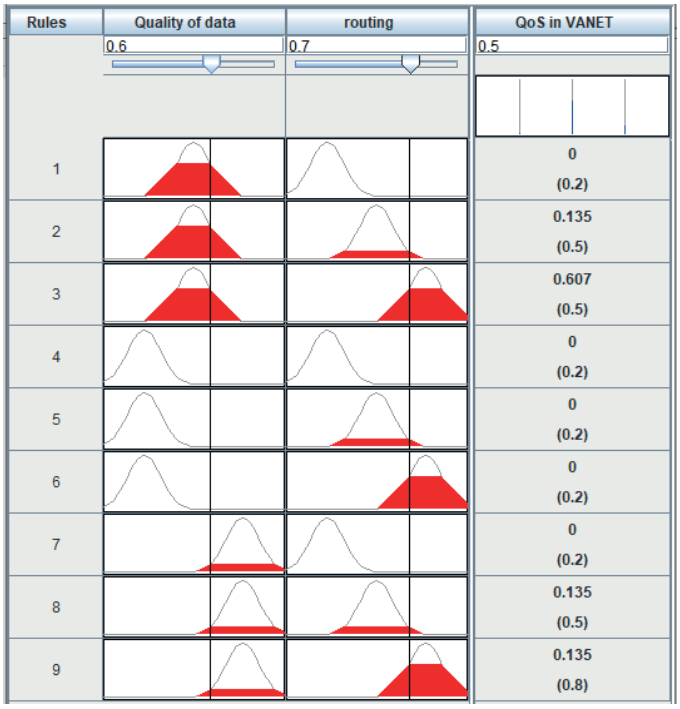


Fig. 4. Fuzzy inference of the 'QoS in VANET' variable.

The next step aggregates different conclusions of the activated rules, as shown in Table V, and combines them into a single value. This value is obtained by the union of all the triggered conclusions, translated by the max operator.

TABLE V
THE ACTIVATED RULES OF THE "QOS IN VANET"

ACTIVATED RULES	LINGUISTIC VALUE FOR THE OUTPUT	DEGREE OF APPURTENANCE
R2	medium	0.135
R3	medium	0.607
R8	medium	0.135
R9	good	0.135

[3] https://www.fispro.org/en/

The 'medium' and 'good' values of the variable 'QoS in VANET' are 0.607 and 0.135, respectively. However, the lowest value of 0.001 is tolerated in the case where the possibility is zero (here for the 'bad value') since each state of the variable 'QoS in VANET' is possible, and this possibility must be greater than zero.

QoS in VANET (bad) = 0.001

QoS in VANET (medium) = max (0.607, 0.135, 0.135) = 0.607

QoS in VANET (good) = 0.135

The sum of probabilities for each variable states must be equal to 1. The CPs for the different states of the variable 'QoS in VANET' of rule number 3 are calculated as follows:

P (QoS in VANET = bad | data quality = medium, routing = high) = 0.001/ (0.001+0.607+0.135) = 0.001

P (QoS in VANET = medium | data quality = medium, routing = high) = 0.607/ (0.001+0.607+0.135) = 0.817

P (QoS in VANET = good | data quality = medium, routing = high) = 0.135/ (0.001+0.607+0.135) = 0.182

By following this approach, all CPs for the variable 'QoS in VANET' for the different states of its antecedents were computed as presented in Table VI.

TABLE VI

CPS TABLE OF THE VARIABLE "QOS IN VANET"

			QOS IN VANET		
RULE	QUALITY OF DATA	ROUTING	BAD	MEDIUM	GOOD
1	medium 0.56	bad 0.17	0.994	0.005	0.001
2	medium 0.56	Medium 0.57	0.002	0.931	0.067
3	medium 0.56	good 0.88	0.003	0.926	0.071
4	bad 0.22	bad 0.17	0.995	0.004	0.001
5	bad 0.22	medium 0.57	0.975	0.023	0.001
6	bad 0.22	good 0.88	0.972	0.027	0.001
7	good 0.77	bad 0.17	0.995	0.004	0.001
8	good 077	medium 0.57	0.002	0.935	0.063
9	good 0.77	good 0.88	0.001	0.035	0.964

V. DISCUSSION

The proposed FB model predicts the QoS state in VANET. By varying the values of the input parameters, their effects on the different nodes of the graph are estimated, implementing the fuzzy inference method.

In many domains and studies, the combination of the BN and the FL system is used, for example, predicting the population status of a rare animal using the inference mechanism in the ecological domain [54], determining the severity scale of a disease based on fuzzy medical rules [55], predicting the risks of delays in deliveries in logistic services [56] and others.

To our knowledge, no prior work analyses risks in VANETs and predicts QoS, considering all previously mentioned parameters, which justifies the interest and originality of the research presented in this article. In addition, this study provides an approach for generating massive data that help in making decisions in the transportation domain. Some classical approaches and existing studies give optimal solutions to improve QoS in VANET but can only consider a few parameters simultaneously. However, in reality, where decisions have to be made based on several criteria, these approaches are insufficient. Consequently, the presented approach is fruitful. It allows risk analysis at any time in the network and provides a massive database that can be extended progressively using deep learning techniques.

VI. CONCLUSION

One unknown problem can perturb the communication system or block the proper functioning of the network, causing material and human losses. For that reason, equipping with risk prediction tools is very important. This article proposes a FB model combining the BN approach that evaluates the causality relation between its nodes based on different data resources, such as expert estimations or learning databases, and FL used to generate all CPs needed. This model allows calculating the QoS in VANET in the function of multiple criteria and provides a database that helps determine the originality of risk degrading the QoS in the network. The complexity of the proposed approach consists of the integration of all the factors that influence the QoS in VANET, where the absence of some variables can affect the efficacy of the prediction.

The future work will complete the actual model by generating the CPs of all nodes in the causal graph and propose some scenarios for proving the model efficacy. Furthermore, some solutions will be presented in the case of bad QoS in the network.

ACKNOWLEDGEMENT

The research has been supported by the Ministry of Higher Education, Scientific Research and Innovation, the Digital Development Agency (DDA) and the National Centre for Scientific and Technical Research (CNRST) of Morocco (Smart DLSP Project – AL KHAWARIZMI IA-PROGRAM).

REFERENCES

[1] R. Bibi, Y. Saeed, A. Zeb, T. M. Ghazal, T. Rahman, R. A. Said, S. Abbas, M. Ahmad, and M. A. Khan, "Edge AI-based automated detection and classification of road anomalies in VANET using deep learning," *Computational Intelligence and Neuroscience*, vol. 2021, Art. no. 6262194, Sep. 2021. https://doi.org/10.1155/2021/6262194

[2] M. Gayathri and C. Gomathy, "A deep survey on types of cyber attacks in VANET," *J Crit Rev*, vol. 8, no. 1, pp. 1029–1039, 2021. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.jcreview.com/admin/Uploads/Files/61c07bf6658ea1.10579682.pdf

[3] S. Lahdya and T. Mazri, "Security study of routing attacks in vehicular ad-hoc networks (autonomous car)," *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 46, pp. 349–353, 2021. https://doi.org/10.5194/isprs-archives-XLVI-4-W5-2021-349-2021

[4] A. E. C. Mondragon, C. S. Lalwani, E. S. C. Mondragon, and C. E. C. Mondragon, "Facilitating multimodal logistics and enabling information systems connectivity through wireless vehicular networks," *International Journal of Production Economics*, vol. 122, no. 1, pp. 229–240, Nov. 2009. https://doi.org/10.1016/j.ijpe.2009.05.023

[5] J. I. Katuka and M. S. A. Latiff, "VANETs and its related issues: An extensive survey," *Journal of Theoretical & Applied Information Technology*, vol. 66, no. 1, pp. 693–697, 2014.

[6] P. Pandey, "Effect of selfish behavior on network performance in VANET," in *Fifth International Conference on Communication Systems and Network Technologies*, Gwalior, India, Apr. 2015, pp. 693–697. https://doi.org/10.1109/CSNT.2015.63
[7] S. Harrabi, I. B. Jaafar, and K. Ghedira, "Performance analysis of VANETs routing protocols," Res. Square, Univ. Mannouba, Manouba, Tunisia, Tech. Rep., 2021.
[8] E. Singh, "Mobility and scalability management issues in VANET," *Int J Adv Res Sci Eng*, vol. 7, pp. 151–155, 2018.
[9] A. Ahamed and H. Vakilzadian, "Issues and challenges in VANET routing protocols," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, Rochester, MI, USA, May 2018, pp. 723–728. https://doi.org/10.1109/EIT.2018.8500180
[10] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in VANETs," *Computer Science Review*, vol. 41, Art. no. 100411, Aug. 2021. https://doi.org/10.1016/j.cosrev.2021.100411
[11] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An efficient authentication scheme based on semi-trusted authority in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2972–2986, Mar. 2019. https://doi.org/10.1109/TVT.2019.2896018
[12] A. Quyoom, A. A. Mir, and A. Sarwar, "Security attacks and challenges of VANETs: a literature survey," *Journal of Multimedia Information System*, vol. 7, no. 1, pp. 45–54, Mar. 2020. https://doi.org/10.33851/JMIS.2020.7.1.45
[13] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Vehicular Communications*, vol. 19, Art. no. 100179, Oct. 2019. https://doi.org/10.1016/j.vehcom.2019.100179
[14] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting dos attacks in VANETs," *IEEE Access*, vol. 5, pp. 24012–24022, 2017. https://doi.org/10.1109/ACCESS.2017.2768499
[15] I. A. Sumra, H. B. Hasbullah, and J.-l. B. AbManan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey," in *Vehicular Ad-Hoc Networks for Smart Cities*, vol. 306, A. Laouiti, A. Qayyum, M. S. Mohamad, Eds. Springer, Singapore, 2015, pp. 51–61. https://doi.org/10.1007/978-981-287-158-9_5
[16] R. Kaur, T. P. Singh, and V. Khajuria, "Security issues in vehicular Ad-hoc network (VANET)," in *2018 2nd International conference on trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, May 2018, pp. 884–889. https://doi.org/10.1109/ICOEI.2018.8553852
[17] M. Azees, P. Vijayakumar, and L. Jegatha Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379–388, Aug. 2016. https://doi.org/10.1049/iet-its.2015.0072
[18] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, Apr. 2014. https://doi.org/10.1016/j.vehcom.2014.05.001
[19] J. Contreras-Castillo, S. Zeadally, and J. A. G Ibañez, "Solving vehicular *ad hoc* network challenges with big data solutions," *IET Networks*, vol. 5, no. 4, pp. 81–84, Jul. 2016. https://doi.org/10.1049/iet-net.2016.0001
[20] A. Mchergui, T. Moulahi, and S. Zeadally, "Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (VANETs)," *Vehicular Communications*, vol. 34, Art. no. 100403, Apr. 2021. https://doi.org/10.1016/j.vehcom.2021.100403
[21] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Challenges of future VANET and cloud-based approaches," *Wireless Communications and Mobile Computing*, vol. 2018, Art. no. 5603518, May 2018. https://doi.org/10.1155/2018/5603518
[22] M. Pourkiani, S. Adabi, S. Jabbehdari, and A. Khademzadeh, "Improving QoS in VANETs: A survey," *Journal of Advances in Computer Engineering and Technology*, vol. 3, no. 3, pp. 153–166, 2017.
[23] M. Pourkiani, S. Jabbehdari, and A. Khademzadeh, "A novel protocol stack for improving QoS in vehicular networks," *International Journal of Computer Science and Information Security*, vol. 14, no. 6, pp. 358– 367, June 2016.
[24] H. Fatemidokht and M. K. Rafsanjani, "QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks," *Journal of Systems and Software*, vol. 165, Art. no. 110561, Jul. 2020. https://doi.org/10.1016/j.jss.2020.110561
[25] A. Srivastava, S. Verma, N. Jhanjhi, M. Talib, A. Malhotra *et al.*, "Analysis of quality of service in VANET," *IOP Conference Series: Materials Science and Engineering,* vol. 993, no. 1, Art. no. 012061, 2020. https://doi.org/10.1088/1757-899X/993/1/012061
[26] S. Tabar and A. Azadmanesh, "Quality of service in vehicular ad hoc networks," in *IAENG Transactions on Engineering Sciences: Special Issue for the International Association of Engineers Conferences 2016*, World Scientific, 2018, pp. 388–401. https://doi.org/10.1142/9789813230774_0028
[27] P. D. Dorge, S. S. Dorle, M. B. Chakole, and D. K. Thote, "Improvement of QoS in VANET with different mobility patterns," in *International Conference on Radar, Communication and Computing (ICRCC)*, Tiruvannamalai, India, Dec. 2012, pp. 206–209. https://doi.org/10.1109/ICRCC.2012.6450578
[28] G. Parimala, S. Nageswararao, and K. LakshmiNadh, "Ddsrc: Algorithm for improving QoS in VANET," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 7, no. 6S5, pp. 1327–1331, Apr. 2019.
[29] M. J. Sayadi, M. Fathy, and L. Mahaki, "Improving the quality of service in the VANET by detecting and removing unused messages," *International Journal of Information & Communication Technology Research*, vol. 4, no. 3, pp. 107–112, 2012.
[30] N. K. Kitson, A. C. Constantinou, Z. Guo, Y. Liu, and K. Chobtham, "A survey of Bayesian network structure learning," *arXiv preprint, arXiv:2109.11415*, 2021. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://arxiv.org/ftp/arxiv/papers/2109/2109.11415.pdf
[31] M. Scanagatta, A. Salmeron, and F. Stella, "A survey on Bayesian network structure learning from data," *Progress in Artificial Intelligence*, vol. 8, no. 4, pp. 425–439, May 2019. https://doi.org/10.1007/s13748-019-00194-y
[32] N. R. Siddiqui, K. A. Khaliq, and J. Pannek, "VANET security analysis on the basis of attacks in authentication," in *Dynamics in Logistics*, *Lecture Notes in Logistics*, M. H. Kotzab and J. Pannek, Eds. Springer, 2017, pp. 491–502. https://doi.org/10.1007/978-3-319-45117-6_43
[33] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures," *arXiv preprint, arXiv:1903.01541*, 2019. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://arxiv.org/ftp/arxiv/papers/1903/1903.01541.pdf
[34] M. B. Mansour, C. Salama, H. K. Mohamed, and S. A. Hammad, "VANET security and privacy-an overview," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 10, no. 2, Mar. 2018. https://doi.org/10.2139/ssrn.3290553
[35] G.-U. Rehman, A. Ghani, S. Muhammad, M. Singh, and D. Singh, "Selfishness in vehicular delay-tolerant networks: A review," *Sensors*, vol. 20, no. 10, Art. no. 3000, 2020. https://doi.org/10.3390/s20103000
[36] A. Reyes, C. Barrado, M. Lopez, and C. Excelente, "Vehicle density in VANET applications," *Journal of Ambient Intelligence and Smart Environments*, vol. 6, no. 4, pp. 469–481, 2014. https://doi.org/10.3233/AIS-140271
[37] A. V. Ostroukh and H. Elhadi, "Comparative study of routing protocols in vehicular ad-hoc networks (VANETs)," *International Journal of Advanced Studies (iJAS)*, vol. 4, no. 2, pp. 9–14, 2014. https://doi.org/10.12731/2227-930X-2014-2-2
[38] C. Tripp-Barba, M. A. Igartua, L. U. Aguiar, A. M. Mezher, A. Zaldívar-Colado, and I. Guerin-Lassous, "Available bandwidth estimation in GPSR for VANETs," in *Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications*, Nov. 2013, pp. 1–8. https://doi.org/10.1145/2512921.2516961
[39] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control," *IEEE transactions on systems, man, and cybernetics*, vol. SMC-15, no. 1, pp. 116–132, Jan.-Feb. 1985. https://doi.org/10.1109/TSMC.1985.6313399
[40] K. A. Hafeez, L. Zhao, Z. Liao, and B. N.-W. Ma, "The optimal radio propagation model in VANET," in *2009 Fourth International Conference on Systems and Networks Communications*. Porto, Portugal, Sep. 2009, pp. 6–11. https://doi.org/10.1109/ICSNC.2009.101
[41] F. Li, W. Chen, and Y. Shui, "Study on connectivity probability of VANETs under adverse weather conditions at 5.9 Ghz," *IEEE Access*, vol. 8, pp. 547–555, Dec. 2019. https://doi.org/10.1109/ACCESS.2019.2962089
[42] M. C. Surugiu and I. N. Stancel, "Monitoring and warning system of a route based on roadside sensors in VANET," *Procedia Manufacturing*, vol. 32, pp. 745–752, 2019. https://doi.org/10.1016/j.promfg.2019.02.281
[43] S. Abdelhamid, H. S. Hassanein, and G. Takahara, "Vehicle as a resource (VaaR)," *IEEE Network*, vol. 29, no. 1, pp. 12–17, Jan. 2015. https://doi.org/10.1109/MNET.2015.7018198

[44] N. Mohamed, S. Sahib, N. Suryana, and B. Hussin, "Understanding network congestion effects on performance-articles review," *Journal of Theoretical and Applied Information Technology*, vol. 92, no. 2, Art. no. 311, 2016.

[45] R. Chen, Z. Sheng, Z. Zhong, M. Ni, D. G. Michelson, and V. C. Leung, "Analysis on connectivity performance for vehicular ad hoc networks subjected to user behavior," in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*. Dubrovnik, Croatia, Aug. 2015, pp. 26–31. https://doi.org/10.1109/IWCMC.2015.7288932

[46] R. K. Aswed and M. A. Abdala, "End-to-end delay enhancement with aodv in VANET," *International Journal of Enhanced Research in Science, Technology & Engineering*, vol. 3, no. 11, pp. 227–232, Nov. 2014,

[47] S. Renooij, "Probability elicitation for belief networks: issues to consider," *The Knowledge Engineering Review*, vol. 16, no. 3, pp. 255–269, Feb. 2001. https://doi.org/10.1017/S0269888901000145

[48] H. Sattar, I. S. Bajwa, J. Muhammad, M. F. Mushtaq, R. Kazmi, M. Akram, M. Ashraf, U. Shafi *et al.*, "Smart wound hydration monitoring using biosensors and fuzzy inference system," *Wireless Communications and Mobile Computing*, vol. 2019, Art. no. 8059629, 2019. https://doi.org/10.1155/2019/8059629

[49] M.-D. Pop, O. Prostean, T.-M. David, and G. Prostean, "Hybrid solution combining Kalman filtering with Takagi–Sugeno fuzzy inference system for online car-following model calibration," *Sensors*, vol. 20, no. 19, Art. no. 5539, Sep. 2020. https://doi.org/10.3390/s20195539

[50] E. H. Mamdani and S. Assilian, "An experiment in linguistic synthesis with a fuzzy logic controller," *International Journal of Man-Machine Studies*, vol. 7, no. 1, pp. 1–13, 1975. https://doi.org/10.1016/S0020-7373(75)80002-2

[51] M. H. Rad and M. Abdolrazzagh-Nezhad, "Data cube clustering with improved DBSCAN based on fuzzy logic and genetic algorithm: Designing and improving data cube clustering," *Information Technology and Control*, vol. 49, no. 1, pp. 127–143, Mar. 2020. https://doi.org/10.5755/j01.itc.49.1.23780

[52] A. Omar, A. Aous, A. Ali, and S. S. Balasem, "Comparison between the effects of different types of membership functions on fuzzy logic controller performance," *International Journal of Emerging Engineering Research and Technology*, vol. 76, pp. 76–83, 2015.

[53] S. N. Mandal, J. P. Choudhury, and S. B. Chaudhuri, "In search of suitable fuzzy membership function in prediction of time series data," *International Journal of Computer Science Issues*, vol. 9, no. 3, pp. 293–302, 2012.

[54] K.-R. Liu, J.-Y. Kuo, K. Yeh, C.-W. Chen, H.-H. Liang, and Y.-H. Sun, "Using fuzzy logic to generate conditional probabilities in Bayesian belief networks: a case study of ecological assessment," *International Journal of Environmental Science and Technology*, vol. 12, no. 3, pp. 871–884, Dec. 2015. https://doi.org/10.1007/s13762-013-0459-x

[55] V. Zarikas, E. Papageorgiou, and P. Regner, "Bayesian network construction using a fuzzy rule based approach for medical decision support," *Expert Systems*, vol. 32, no. 3, pp. 344–369, Jun. 2015. https://doi.org/10.1111/exsy.12089

[56] O. E. Bouhadi, M. Azmani, A. Azmani, and M. A. el ftouh, "Using a fuzzy-Bayesian approach for predictive analysis of delivery delay risk," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 7, pp. 316–326, 2022. https://doi.org/10.14569/IJACSA.2022.0130740



Hafida Khalfaoui obtained her B.Sc. in Electronic and Telecommunication Engineering and her M.Sc. in Telecommunication Systems and Computer Networks from Sultan Moulay Slimane University, Beni Mellal, Morocco, in 2017 and 2019, respectively. She is following her PhD in Mathematics and Computer Science at Sultan Moulay Slimane University. Her research interests include computer science and network security.
E-mail: hafidakhalfaoui1996@gmail.com
ORCID iD: https://orcid.org/0000-0002-9408-1301



Abdellah Azmani received his PhD degree in Industrial Computing in Dynamic System Modelling and Artificial Intelligent at the University of Science and Technology of Lille in 1991. He worked as a Professor at the Ecole Centrale of Lille, France and at the Institute of Computer and Industrial Engineering from Lens, France. He is a Professor at the Faculty of Science and Technology of Tangier, Morocco. He is a member of the Laboratory of Informatics, System and Telecommunication (LIST) and he created the Intelligent Automation team, which he coordinates. He has contributed to many theses, scientific research projects and he elaborates and produces many IT and decision support solutions for public administration, business management, marketing and logistics.
E-mail**:** a.azmani@uae.ac.ma
ORCID iD: https://orcid.org/0000-0003-4975-3807



Abderrazak Farchane received his B.Sc. in Computer Science and Engineering in June 2001 and M.Sc. in Computer Science and Telecommunication from the University of Mohammed V Agdal, Rabat, Morocco, in 2003. He obtained his PhD in Computer Science and Engineering at ENSIAS, Rabat, Morocco. He is currently an Associate Professor of Computer Science at the Polydisciplinary Faculty, Sultan Moulay Slimane University, Morocco. His areas of interest are information coding theory, cryptography, and security.
E-mail: a.farchane@gmail.com



Said Safi received his B.Sc. degree in Electronics from Cadi Ayyad University, Marrakech, Morocco, in 1995. He obtained his M.Sc. and PhD from Chouaib Doukkali University and Cadi Ayyad University in 1997 and 2002, respectively. He is currently a Professor of Science at the Multidisciplinary Faculty, Sultan Moulay Slimane University, Beni Mellal, Morocco. His general interests span the areas of communications and signal processing, estimation, time-series analysis and system identification.
Safi has more than 160 publications. His research currently focuses on transmitter and receiver diversity techniques for single and multi-user fading communication channels and on broadband wireless communication systems.
E-mail: safi.said@gmail.com
ORCID iD: https://orcid.org/0000-0003-3390-9037